SPYWOLF

Security Audit Report

Completed on

January 20, 2023

OVERVIEW

This audit has been prepared for **Howl Finance** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

HOWL FINANCE

PROJECT DESCRIPTION

According to their whitepaper:

$WOLF brings utility in many forms. Including sustainability, passive income, trust, honesty, NFTs, SaaS and financial freedom! With an ecosystem which provides a great way to gain during any market conditions, we are here through thick and thin.

Utilities list:

- Wolf Swap
- Wolfolio
- SaaS (Software as a Service)
- The Wolf Pack
- The Hunting Grounds

Release Date: Presale starts in January, 2023

Category: Utility token

CONTRACT INFO

Token Name
Howl Finance

Symbol
HOWL

Contract Address
0xf034C80F9a3b6996dC23B17764d03FBC11d294b7

Network
Binance Smart Chain
TESTNET

Language
Solidity

Deployment Date
Jan 19, 2023

Verified?
Yes

Total Supply
1,000,000,000

Status
Not launched

TAXES

Buy Tax
none

Sell Tax
none

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of January 20, 2023)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount

10,000,000

DEX:

PancakeSwap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	TESTNET
Uniq Senders	TESTNET
Uniq Receivers	TESTNET
Total Amount	TESTNET
Median Transfer Amount	TESTNET
Average Transfer Amount	TESTNET
First transfer date	TESTNET
Last transfer date	TESTNET
Days token transferred	TESTNET

SMART CONTRACT STATS

Calls Count	TESTNET
External calls	TESTNET
Internal calls	TESTNET
Transactions count	TESTNET
Uniq Callers	TESTNET
Days contract called	TESTNET
Last transaction time	TESTNET
Created	TESTNET
Create TX	TESTNET
Creator	TESTNET

FEATURED WALLETS

Owner address	0xeeeedba6bfbd03efe1de85988f9db3a1edeafa52
Buyback fee receiver	0xeeeedba6bfbd03efe1de85988f9db3a1edeafa52
LP address	**Liquidity not added yet**

PRESALE STATS (Pinksale)

Total Supply	1,000,000,000 HOWL
Tokens For Presale	N/A
Tokens For Liquidity	N/A
Soft Cap	N/A
Presale Start Time	N/A
Presale End Time	N/A
Listing On	Pancakeswap
Liquidity Percent	N/A
Liquidity Lockup Time	N/A

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can change auto swap threshold.
If swapThrehold is set to very low number, selling will fail.

```
function setSwapBackSettings(bool _enabled, uint256 _amount) external onlyOwner {
    require(_amount > 0, "Amount is zero");
    require(_amount < (_totalSupply/10), "Amount too high");

    swapEnabled = _enabled;
    swapThreshold = _amount;

    emit config_SwapSettings(swapThreshold, swapEnabled);
}
```

- Recommendation:
  - Ensure that the swapThreshold variable is always above 0 (zero) and more precisely equal or above 1 (one) token.
  - Token's decimals should be taken into consideration.
    Example value for 1 (one) token with decimals included:
    10000000000000000

Informational

Owner can set buy/sell fees up to 25% combined.

```
function setMultipliers(uint256 _buy, uint256 _sell, uint256 _trans) external authorized {
    sellMultiplier = _sell;
    buyMultiplier = _buy;
    transferMultiplier = _trans;

    update_fees();
}

function setFees_base1000(uint256 _liquidityFee,  uint256 _marketingFee,
uint256 _buybackFee, uint256 _burnFee) external onlyOwner {
    liquidityFee = _liquidityFee;
    marketingFee = _marketingFee;
    buybackFee = _buybackFee;
    burnFee = _burnFee;
    totalFee = _liquidityFee + _marketingFee + _buybackFee + _burnFee;

    update_fees();
}

function update_fees() internal {
    require(totalFee.mul(buyMultiplier).div(100) <= 200, "Buy tax cannot be more than 20%");
    require(totalFee.mul(sellMultiplier).div(100) <= 200, "Sell tax cannot be more than 20%");
    require(totalFee.mul(sellMultiplier + buyMultiplier).div(100) <= 250, "Buy+Sell tax cannot be more than 25%");
    require(totalFee.mul(transferMultiplier).div(100) <= 150, "Transfer Tax cannot be more than 15%");

    emit UpdateFee( uint8(totalFee.mul(buyMultiplier).div(100)),
        uint8(totalFee.mul(sellMultiplier).div(100)),
        uint8(totalFee.mul(transferMultiplier).div(100))
        );
}
```

Informational

Owner can exclude address from fees, max transaction limit and max wallet limit.

```
function manage_FeeExempt(address[] calldata addresses, bool status) external authorized {
    require(addresses.length < 501,"GAS Error: max limit is 500 addresses");
    for (uint256 i=0; i < addresses.length; ++i) {
        isFeeExempt[addresses[i]] = status;
        emit Wallet_feeExempt(addresses[i], status);
    }
}

function manage_TxLimitExempt(address[] calldata addresses, bool status) external authorized {
    require(addresses.length < 501,"GAS Error: max limit is 500 addresses");
    for (uint256 i=0; i < addresses.length; ++i) {
        isTxLimitExempt[addresses[i]] = status;
        emit Wallet_txExempt(addresses[i], status);
    }
}

function manage_WalletLimitExempt(address[] calldata addresses, bool status) external authorized {
    require(addresses.length < 501,"GAS Error: max limit is 500 addresses");
    for (uint256 i=0; i < addresses.length; ++i) {
        isWalletLimitExempt[addresses[i]] = status;
        emit Wallet_holdingExempt(addresses[i], status);
    }
}
```

Owner can change max transaction limit but cannot lower it than 0.1% of total supply.

```
function setMaxTxPercent_base10000(uint256 maxTXPercentage_base10000) external onlyOwner {
    require(maxTXPercentage_base10000 >= 10,"Cannot set max transaction less than 0.1%");
    _maxTxAmount = (_totalSupply * maxTXPercentage_base10000 ) / 10000;
    emit config_MaxTransaction(_maxTxAmount);
}
```

Informational

Owner can withdraw any tokens from the contract except the native token and bnb token.

```
function clearStuckToken(address tokenAddress, uint256 tokens) external authorized returns (bool success) {
    require(tokenAddress != address(this),"Cannot withdraw native token");
    if(tokenAddress == pair){
        require(block.timestamp > launchedAt + 500 days,"Locked for 1 year");
    }

    if(tokens == 0){
        tokens = BEP20(tokenAddress).balanceOf(address(this));
    }

    emit clearToken(tokenAddress, tokens);

    return BEP20(tokenAddress).transfer(msg.sender, tokens);
}
```

Unused functions

The following variables and functions are not usable and can be deleted from the contract:

```
bool public burnEnabled = false;
uint256 public lastSync;

function disableBurns() external onlyOwner {
    burnEnabled = false;
}

function enableBurns() external onlyOwner {
    burnEnabled = true;
}

/*
function LPBurn(uint256 percent_base10000) public authorized returns (bool){
    require(percent_base10000 <= 1000, "May not nuke more than 10% of tokens in LP");
    require(block.timestamp > lastSync + 5 minutes, "Too soon");
    require(burnEnabled,"Burns are disabled");

    uint256 lp_tokens = this.balanceOf(pair);
    uint256 lp_burn = lp_tokens.mul(percent_base10000).div(10_000);

    if (lp_burn > 0){
        _basicTransfer(pair,DEAD,lp_burn);
        pairContract.sync();
        return true;
    }

    return false;
}
*/
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

HOWL FINANCE

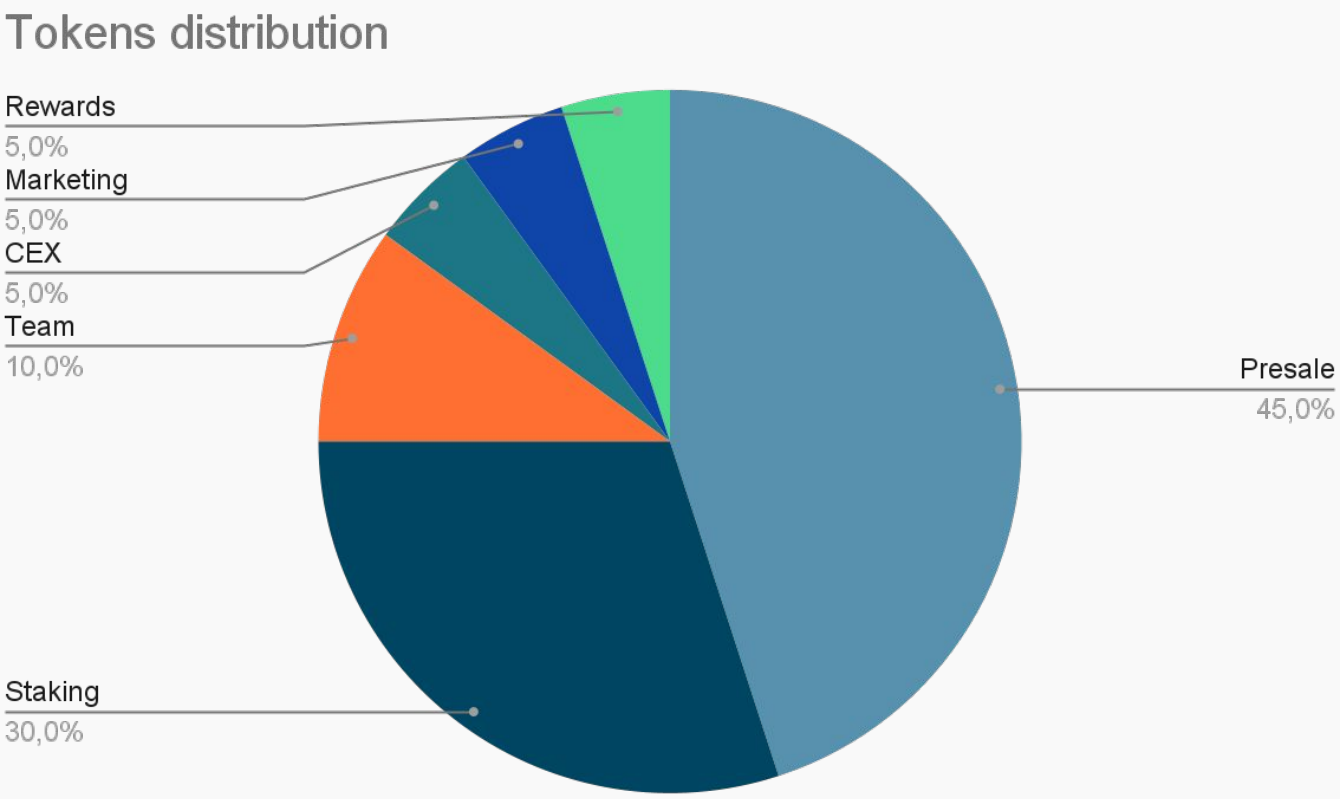
GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner can set a transaction limit, but can’t lower it than 0.1% of total supply
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 45% - Presale
- 30% - Staking
- 10% - Team (vested)
- 5% - CEX
- 5% - Marketing
- 5% - Rewards



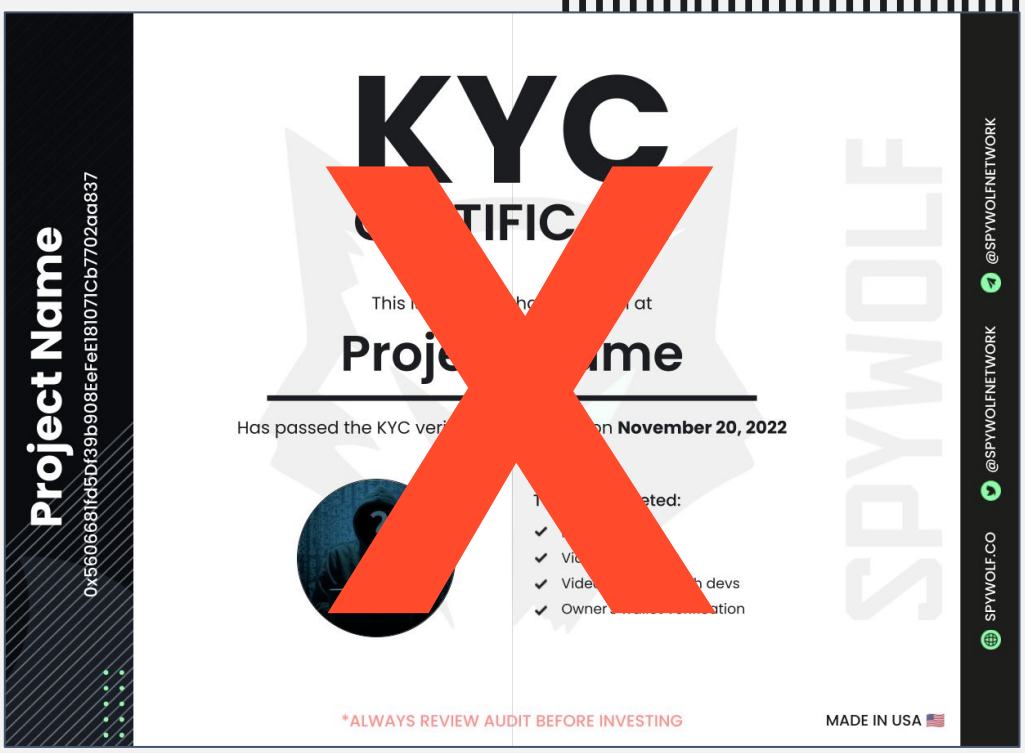
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://www.howlfinance.com/

Domain Registry
https://www.wix.com

Domain Expiration
2023-12-22

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

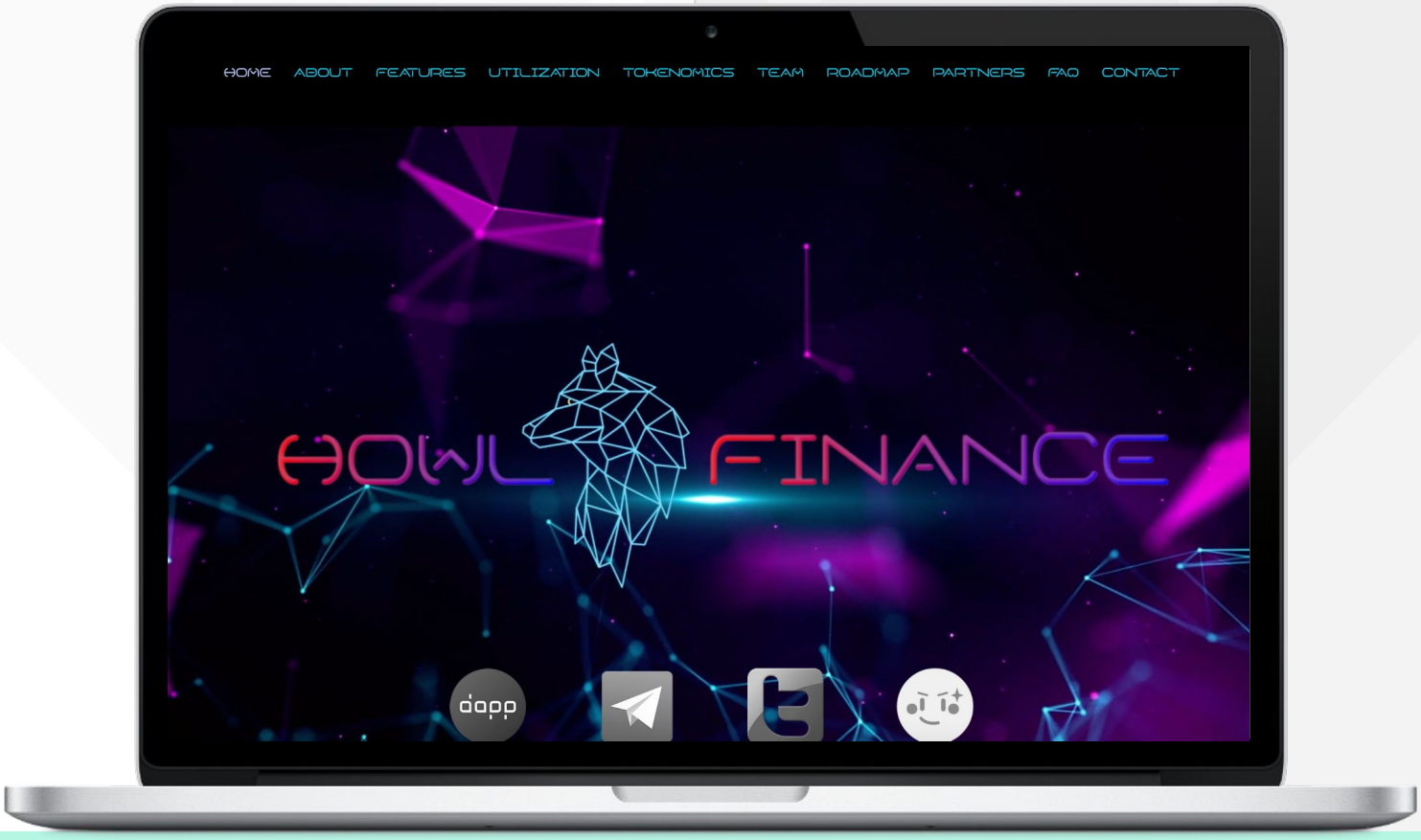
Design
Single page design with nice color scheme and overall layout.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found..

Whitepaper
No whitepaper.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes



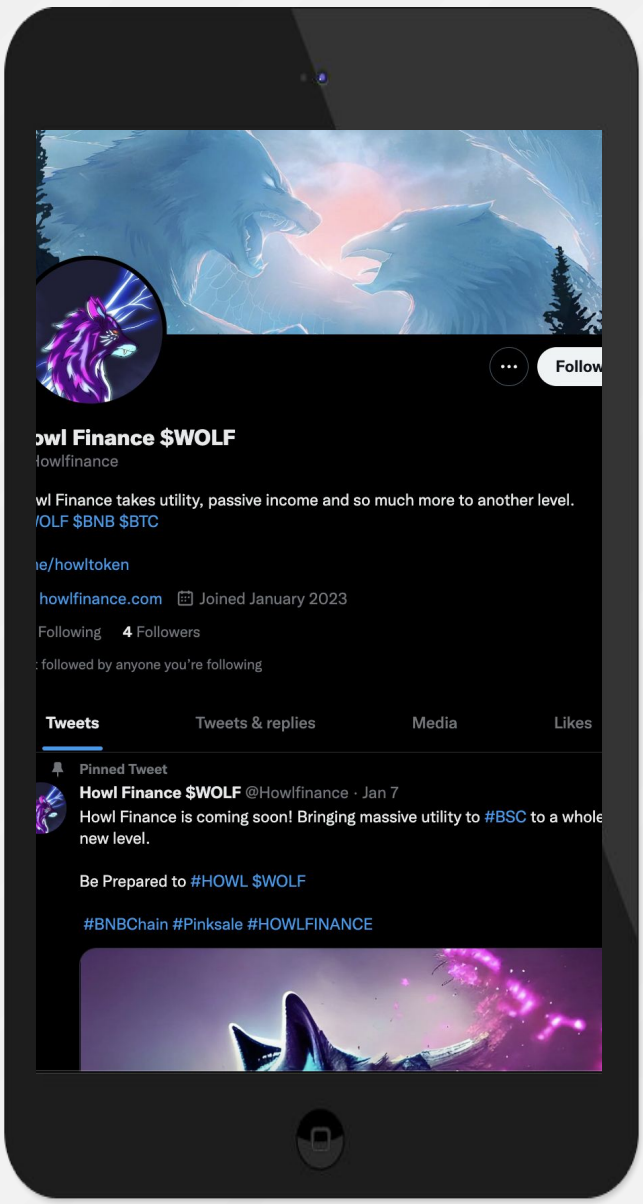
howlfinance.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media presence is concentrated in telegram.



Twitter

@Howlfinance

- 26 followers
- 1 post total

Discord

- Not available

Telegram

@HowlToken

- 243 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.